Guidelines

Internet of Things (IoT) Cyber Security Guide

Annex A
Foundational Concepts

In consultation with:

SG:D
EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

CSA SINGAPORE

IMDA IoT Cyber Security Guide Annex A
Version 1, Mar 2020

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Content

This Guide is a living document which is subject to review and revision periodically.

Guides are informative documents and voluntary in nature except when it is made mandatory by a regulatory authority. It can also be reference in contracts as mandatory requirements. Users are advised to assess the suitability of this guide for their intended use.

Compliance with this guide does not exempt users from any legal obligations.

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE LIABLE FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT THE PRACTICE OR IMPLEMENTATION OF THIS GUIDE MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY CONTRIBUTORS OF THIS DOCUMENT OR ANY THIRD PARTY.

AS OF THE DATE OF THE ISSUANCE OF THE PUBLIC CONSULTATION OF THIS GUIDE, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS GUIDE. HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELATED STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF PATENT RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN LEGAL AND/OR TECHNICAL ADVICE IN RELATION TO THE IMPLEMENTATION OF THE GUIDE IF REQUIRED.

Annex A: Foundational Concepts (informative)

1 Overview

This annex expounds and augments the security concepts introduce in TR64. The concepts provide the foundation for a holistic approach to identify and mitigate the threats and vulnerabilities of IoT systems.

2 Introduction of TR64

This section provides an overview of TR64, and introduces briefly its key concepts and recommendations.

Figure A-1 highlights the scope of TR64.

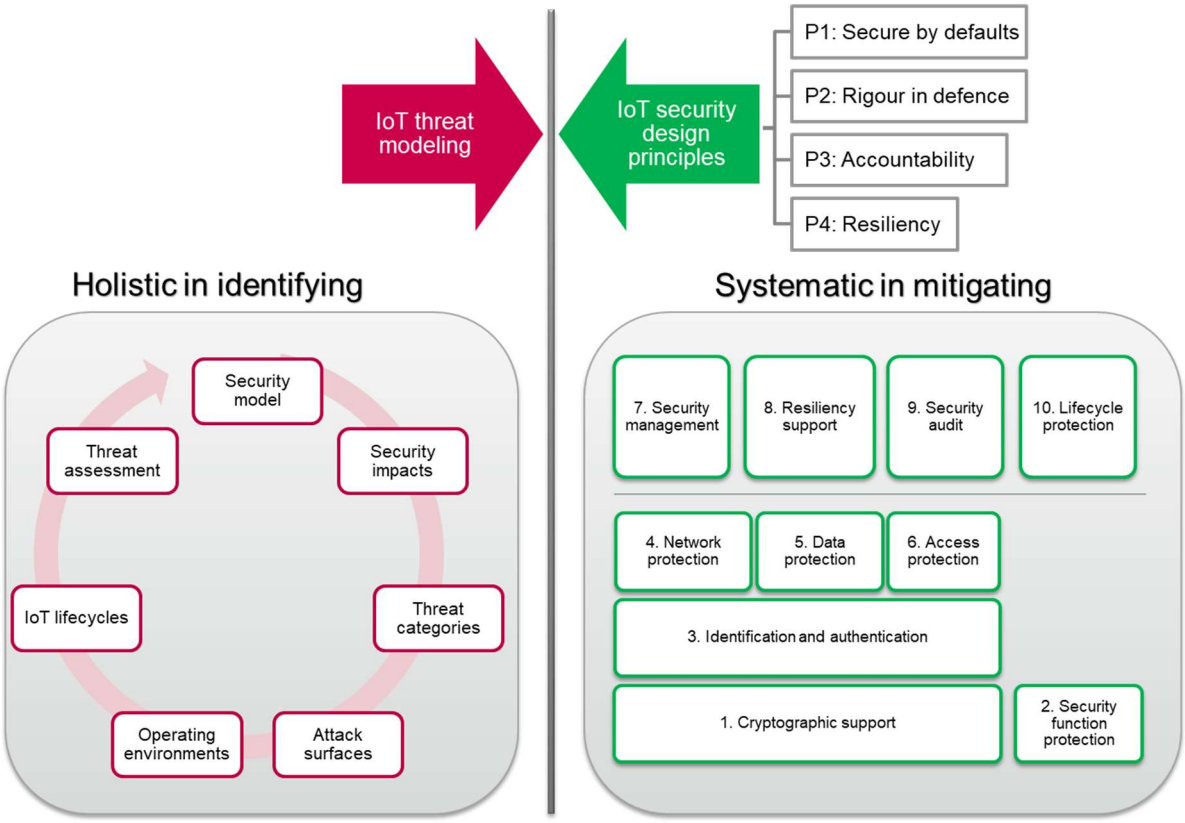


Figure A-1: Highlights of TR64

Firstly, TR64 recommends threat modelling and provides guidance on how to be holistic in identifying and assessing threats specific to IoT systems. In particular, TR64 provides the following:

- A security model that provides guidance to decompose an IoT system into functional layers, cyber and physical.
- Security impact categories for identification of assets of interest based on impacts to security properties, i.e. Confidentiality, Integrity and Availability (**CIA**).

- Threat categories, i.e. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (**STRIDE**) for the enumeration of threats, from both cyber and physical perspectives.

- Attack surface categories that are common to IoT devices.

- Operating environments that IoT devices typically operate in.

- System and device lifecycles with different threat considerations.

- Assess likelihood of threats based on system susceptibility, system accessibility and attacker capability.

Next, TR64 provides four IoT security design principles; distil from well-known best practices, as follows:

- **"Secure by defaults"** recommends making secure choices and ensuring proper configurations. Examples include:

  - Minimising attack surfaces;

  - Establish secure defaults;

  - System hardening;

  - Reducing exposure time.

- **"Rigour in defence"** recommends careful considerations and thoroughness in securing IoT systems. Examples include:

  - Defence in depth (multilayer);

  - Defence in breadth (variety), protect uniformly;

  - Compartmentalisation of system (e.g. network segmentation, micro segmentation);

  - Using encapsulation to manage access to functions;

  - Monitoring, detection and reporting of anomalies, including the use of honey pots;

  - Vulnerability assessment and pen testing;

  - Using a secure engineering approach;

  - Secure system lifecycle;

  - Patch diligently.

- **"Accountability"** recommends controlled access to the IoT systems and proper management of access throughout the system lifecycles. Examples include:

  - Connecting carefully and deliberately;

  - Ensuring the segregation of duties;

  - Establishing and protecting audit trails;

  - Practicing transparency (e.g. vendor disclosure, breach disclosure).

- **"Resiliency"** recommends to be prepare for and recover from the security breach. Examples include:
  - Designing for redundancy;
  - Managing availability;
  - Assumptions of breach;
  - Failing securely (e.g. loss of devices or connectivity);
  - Managing vulnerability;
  - Regular backup and recovery;
  - Testing for scale.

In addition, TR64 defines ten security requirement categories and their relationships, for the systematic mitigation of threats. The order of the categories are significant, where the lower ordered categories typically are the foundation for higher ones. The security of an IoT system is as strong as its weakest links. The ten security requirement categories attempt to highlight the variety of mitigations that requires care in considerations.

3 Security in Context

This section defines security for IoT in the context of Trustworthiness.

Figure A-2 summarises the context of security with respect to attributes of Trust and IoT.

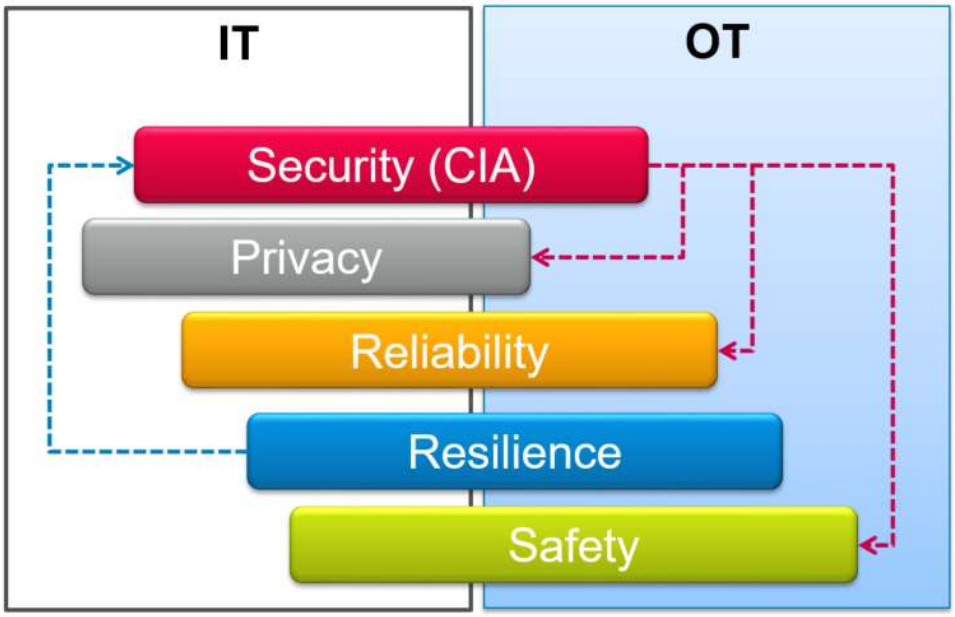


Figure A-2: Security in Context

Firstly, IoT is defined by the combination of two types of subsystem: Information Technology (**IT**) and Operation Technology (**OT**). IT is concerned with interactions of digital aspects only, while OT is concerned with interactions with physical aspects, through sensing and actuation.

Secondly, the trustworthiness of a system can be characterised by its attributes, such as security, privacy, reliability, resilience and safety. IT and OT typically prioritised the attributes of trust differently. IT typically give higher significant to security, privacy and reliability, while OT prioritised safety and resilience.

Lastly, there are relationships between the attributes of trust. Security of a system is characterised by its properties, i.e. CIA and availability-property is impacted by resilience-attribute of trust. In particular, security-attribute impacts privacy, reliability and safety attributes of trust.

4 CIA triad for IT and OT

This section describes how and where CIA triad is applicable for IoT. The concepts of CIA triad are now applied to devices, sensing and actuation, in addition to data and information.

Figure A-3 depicts how CIA triad are applied differently for IT and OT.

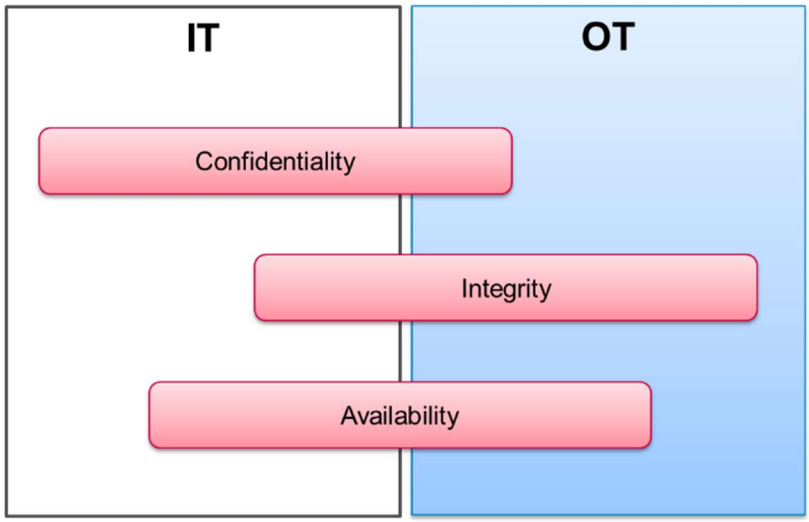


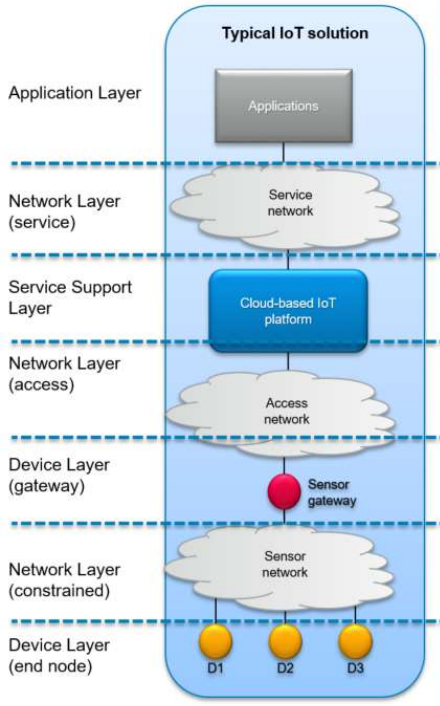
Figure A-3: CIA triad for IT and OT

IT and OT have different emphasis on the CIA triad. In general, IT places more importance in confidentiality-property, while OT put more emphasis on integrity-property because of safety considerations.

5 CIA triad for a typical IoT solution

This section describes where and why CIA triad is applicable for assessing the security needs of a typical IoT solution.

Table A-1 demonstrates the applicability of CIA against the functional layers of a typical IoT solution.



	Confidentiality	Integrity	Availability
Application Layer	x	x	(x)
Network Layer (service)	x	x	x
Service Support Layer	x	x	x
Network Layer (access)	(x)	x	x
Device Layer (gateway)	x	x	x
Network Layer (constrained)	(x)	x	(x)
Device Layer (end node)	(x)	x	(x)

Legend: x = recommended, (x) = optional

Table A-1: CIA triad for a typical IoT solution

For device layer (end node), “Integrity” is recommended because it is important to be able to trust both the device and data generated. A compromised and connected device can become an attacker vector into the enterprise and/or participates in Distributed Denial of Service (**DDoS**) attacks. “Confidentiality” is optional if the device do not contain sensitive data, while “Availability” is optional, based on the required level of service.

For network layer (constrained), “Integrity” is recommended because it is important to be able to trust both the connections and transmitted data. “Confidentiality” is optional if the device do not contain sensitive data, while “Availability” is limited by constrained network.

For device layer (gateway), “Confidentiality”, “Integrity” and “Availability” are recommended because of the assumption that gateway is not constrained. In fact, gateway should also act as a security gateway for remote access to local sensor network and its devices. It is important for the gateway to establish a secure connection for communication between cloud platform and the devices. In addition, the gateway can also act as an agent for the cloud platform to monitor and track the security status of the connected devices.

For network layer (access), “Integrity” and “Availability” are typically provided for public network service providers, while “Confidentiality” is an add-on function.

For service support layer, “Confidentiality”, “Integrity” and “Availability” are recommended because the cloud platform hosted data from multiple sensor networks and users, where some are probably sensitive.

For network layer (service), “Confidentiality”, “Integrity” and “Availability” are recommended because potentially user and processed data are exchanged over public networks or internet.

For application layer, “Confidentiality” is recommended to safeguard sensitive data in storage and “Integrity” is required to safeguard commands invoked from applications.

6 Threats to CIA triad

This section describes categories of threat that impact CIA triad needs.

Table A-2 identifies what CIA triad are impacted by each threat categories.

Confidentiality	Integrity	Availability	
X	X		Spoofing
	X		Tampering
	X		Repudiation
X			Information disclosure
		X	Denial of Service
X	X		Elevation of Privilege

Legend: x = relevant

Table A-2: Threat categories against CIA triad

TR64 identifies six categories of threat, i.e. STRIDE to a typical IoT solution. “Spoofing” and “Elevation of privilege” threats impact confidentiality and integrity. “Tampering” and “Repudiation” threats impacts “Integrity”. “Information disclosure” threats compromise confidentiality, while “Denial of service” compromise availability. These known relationships help to prioritise threats to mitigate with respect to the relative importance to safeguard the CIA triad for a typical IoT solution.

Examples of cyber and physical threats to the six categories of threat are provided in TR64.

7 CIA triad protection

This section describes the extent that security requirement categories is relevant for mitigating CIA triad needs.

Table A-3 identifies what CIA triad are addressed by each security requirement category.

Confidentiality	Integrity	Availability	
x	x		1. Cryptographic support
x	x		2. Security function protection
x	x	x	3. Identification and authentication
	x	x	4. Network protection
x	x		5. Data protection
x	x	x	6. Access protection
x	x	x	7. Security management
		x	8. Resiliency support
x	x		9. Security audit
x	x	x	10. Lifecycle protection

Legend: x = relevant

Table A-3: CIA triad addressed by the different categories of security requirement

Security requirements under the categories of “Cryptographic support”, “Security function protection”, “Data protection” and “Security audit” are most relevant for addressing confidentiality and integrity needs but not availability. Working together, the preceding security requirements categories provide confidence that sensitive data are secured from disclosure and modifications.

Security requirements under the categories of “Identification and authentication”, “Access protection”, “Security management” and “Lifecycle protection” are most relevant for all CIA triad. Security requirements under “Identification and authentication” established trust in the identity of counterparties and also ensure the availability of this service. Security requirements under “Security management” provide confidence in the management of security features, which include anti-malware, proper access control, and secure remote management for devices. Security requirements under “Lifecycle protection” helps to secure the system/product for each life stages and continue to remain secure.

Security requirements under “Network protection” category are most relevant for addressing integrity and availability needs but not confidentiality. Security requirements under “Network protection” provides confidence in transport function, by enforcing connections for authorised nodes only and maintaining those connections.

Security requirements under “Resiliency support” category are most relevant for addressing availability. Security requirements under “Resiliency support” provides assurance that the system continue to operate and/or recover after the system is compromised.

8 Usage of AAA concepts

This section describes the extent that Authentication, Authorisation and Accounting (**AAA**) is relevant to the security requirement categories.

Table A-4 identifies which AAA is relevant for each security requirement category.

	Access control		
	Authentication	Authorization	Accounting
1. Cryptographic support		x	
2. Security function protection		x	
3. Identification and authentication	x		
4. Network protection		x	
5. Data protection		x	
6. Access protection	x	x	
7. Security management		x	
8. Resiliency support		x	x
9. Security audit		x	x
10. Lifecycle protection		x	x

Legend: x = relevant

Table A-4: Relationship with AAA

Firstly, “Access control”, by definition, covers “Authentication”, “Authorisation” and “Accounting”.

Secondly, only “Identification and authentication” and “Access protection” categories have specific requirements on “Authentication”, the other security requirement categories depend on “Identification and authentication” and “Access protection” categories for authentication controls.

Thirdly, while all three categories of “Resiliency support, “Security audit” and “Lifecycle protection” have requirements on “Accounting”, they cover different aspects. “Resiliency support” accounts for and limits resource utilisation to ensure availability. “Security audit” accounts for significant events that took place within the system. “Lifecycle protection” accounts for assets and their patch statuses.

Lastly, all categories can have requirements on “Authorisation”, except “Identification and authentication” category.

9 Usage of IoT security design principles

This section illustrates the application of IoT security design principles, introduced by TR64.

Table A-5 illustrates how the IoT security design principles guide the considerations of specific requirements for each security requirement category.

	P1: Secure by defaults	P2: Rigour in defence	P3: Accountability	P4: Resilience
1. Cryptographic support	Use industry accepted cryptographic protocols	Use of symmetric and asymmetric keys for session protection	Proper key management	Use of perfect forward secrecy (PFS) protocols
2. Security function protection	Use security software signing	Use of hardware root-of-trust	Ensure authenticity of security updates	Support remote attestation
3. Identification and authentication	Use mutual authentication	Use of multi-factor authentication	Log authentication failures	Proper identity management
4. Network protection	Connect deliberately	Use of firewalls and VPN	Log authorization failures	Proper network segmentation
5. Data protection	Enable data encryption	Protect data in transit, in use and at rest	Log access to sensitive data	Backup data periodically
6. Access protection	Restrict physical access	Use out-of-band notifications	Log repeated retries	Anti-tamper mechanisms
7. Security management	Enforce strong passwords	Restrict remote access to secure network	Separation of duties for key management	Keep software / firmware updated
8. Resiliency support	Encrypt backups	Employ self-test, error detection and correction	Monitor and detect resource usage	Conduct backup and recovery exercise
9. Security audit	Enable logging	Encrypt log data	Restrict access to logs	Backup log periodically
10. Lifecycle protection	Employ system hardening	Conduct penetration testing	Proper vulnerability disclosure	Sanitise devices before reuse and/or disposal

Table A-5: Usage of IoT design principles

10 Assessment of threats

This section provides a summary of the concepts and their relationships that are relevant for threat assessment.

Figure A-4 illustrates how to assess the threats to an asset.

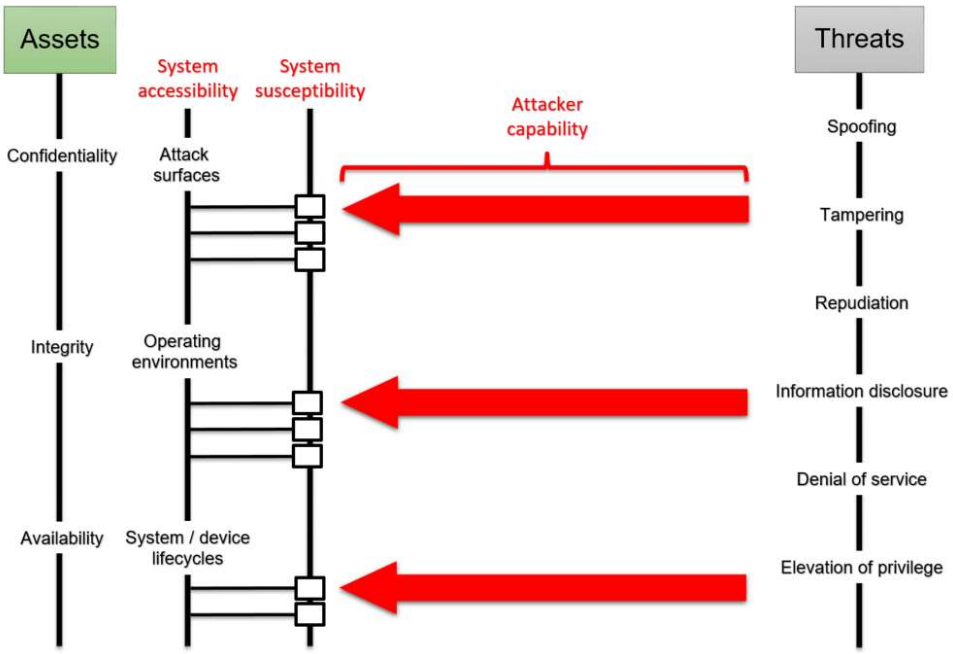


Figure A-4: Assessment of threats

Firstly, threat assessment requires the identification of assets of the system, which is also known as Target Of Protection (**TOP**), and the relative importance of security properties, i.e. CIA triad, to safeguard.

Secondly, accessibility of the system is determined by identifying the attack surfaces, operating environments and system / device lifecycles, exposed by the TOP.

Thirdly, susceptibility of the system is determined by identifying vulnerabilities (starting with known and common vulnerabilities) to the exposed TOP.

Lastly, the attractiveness of the assets to different attacker types (script kiddies, criminals, hacktivist, terrorists, state sponsored, etc) are identified. The attacker types will determine the capability of the attacker to exploit the susceptibility of the system.